UNITED STATES PATENT AND TRADEMARK OFFICE

5

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/678,689	10/03/2000	Graham Arthur Makinson	NAI1P161/00.113.01	6810

28875 7590 03/24/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/678,689	**Applicant(s)** MAKINSON ET AL.	
	Examiner Taghi T. Arani	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-11,13,24-32,34-43,45-53 and 55-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-11,13,24-32,34-43,45-53 and 55-63* is/are rejected.

7)☒ Claim(s) *64-66* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-63 were originally pending.

Claims 2, 12, 23, 33, 44 and 54 are cancelled.

Claims 64-66 are newly added.

Claims 1, 3-11, 13-22, 24-32, 34-43, 45-53, 55-66 are pending.

Response to Amendment

2. Applicant's amendment filed 1/10/2005 necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1, 3, 21, 22, 24, 42, 43, 45, and 63** rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,724,425 to Chang and further in view of US Patent No. 5,113,518 to Durst, Jr. et al. (hereinafter " Durst).

Chang teaches a method and apparatus utilizing public key encryption techniques for enhancing software security and for distributing software (Column 3 Line 15). Chang further teaches that the present invention may be implemented in software executed by computer (Column 6 Line 17).

As per claims 1, 22, and 43, Chang teaches:

reading module signature data associated with said additional computer program module [Chang teaches a step where the computing platform determines if the software passport includes an application writer's license, and if it does, the hardware platform extracts the application writer's license from the passport and determines whether or not the passport includes the platform builder's signature. The signature is then decrypted using the public key provided in the platform (Column 4 Line 17)];

reading core signature data and other signature data associated with said core computer program;

comparing said module signature data with said core signature data and said other signature data [Chang teaches a step where the computing platform recomputes the message digest of the application writer's license and compares the received message digest with the recomputed message digest ;Column 4 Line 25). Chang further teaches that if the digests are equal then the hardware platform extracts the application writer's public key from the application writer's license and extracts the application writer's digital signature (Column 4 Line 29). Chang continues on and states that the hardware platform recomputes the message digest of the binary code comprising the application to be executed and decrypts the application writer's digital signature using the application writer's public key, and then compares the recomputed message digest for the binary code with the application writer's decrypted signature (Column 4 Line 32)];

refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data [Chang teaches that if the recomputed message digest and received message digest are not equal, then the software passport is not genuine and is rejected (Column 4

Line 27). Chang further teaches that if the recomputed message digest for the binary code and the application writer's decrypted signature are equal then the binary code is executed by the platform (Column 4 Line 39);

Chang fails to teach wherein said other signature data is user signature data;

wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program,

However, Durst teaches user signature data , wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program [abstract, col. 3, lines 35-67, i.e. " signature of one or more authorized computer systems is determined and stored , and the, prior to executing a particular program intended to be installed in a computer system, the stored signature is compared to the signature of the computer system intended to be used],

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Chang with the teaching of Durst to prevent computer program from being used by an unauthorized computer system [col. 1, lines 5-13].

As per claims 3, 24, and 45, Chang as modified teaches wherein said addition computer program module is refused authorization for use with said core computer program unless said module signature matches both of said core signature data and said user signature data [Chang teaches that if the recomputed message digest and received message digest are not equal, then the software passport is not genuine and is rejected (Column 4 Line 27). Chang further teaches that if the recomputed message digest for the binary code and the application writer's decrypted signature are equal then the binary code is executed by the platform (Column 4, line 39)].

As per claims 21, 42, and 63, Chang as modified teach writing said additional computer program module [Chang teaches a set of application writers who are authorized to write application code for a particular platform [(Column 8 Line 67). Chang further teaches a software produced by a licensed application writer];

providing said additional computer program module to a new user [Chang teaches that the software: passport is then distributed to a user using any number of software distribution models known in the industry (Column 3 Line 35)];

said new user associating user signature data with said additional computer program module [Chang teaches that the digital signature of the application writer is produced and embedded in the passport].

providing said additional computer program module and associated user signature data to a provider of said core computer program" Chang teaches a first computer which is provided with source code to be protected. In addition the first computer is provided with the software application writer's private key along with an application writer's license (Column 3 Line 18). The application writer's license includes identifying information such as the application writer's name as well as the application writer's public key (Column 3 Line 23).

said provider of said core computer program associating core signature data with said additional computer program module and associated user signature data [Chang teaches that the first computer encrypts the message digest using the application writer's private key such that the encrypted message digest is defined as a digital signature of the application writer (Column 3 Line 29)].

4. **Claims 1, 4, 22, 25, 43, and 46** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,311,591 to Fischer in view of US Patent No. 5,113,518 to Durst, Jr. et al. (hereinafter " Durst).

Fischer teaches a method and apparatus for providing digital information with, enhanced security and protection (Column 1 Line 16).

As per claims 1, 22, and 43, Fischer teaches

reading module signature data associated with said additional computer program module;

reading core signature data and other signature data associated with said core computer program;

comparing said module signature data with said core signature data and said other signature data;

refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data;

Fischer teaches an apparatus that utilizes a unique operating system design that includes a system monitor which limits the ability of a program about to be executed to the use of predefined resources (Column 2 Line 13). Fischer further teaches that the programs about to be executed are digitally signed by some entity that the user trusts and that signature is verified to ensure that the program is trusted and has not been tampered with (Column 2 Line 54). Fischer additionally states that if block 306 indicates that there is a digital signature from the manufacturer in block 308, then the manufacturer's pedigree will be verified by verifying the digital signature and performing whatever certification and authorization checks are appropriate

(Column 16 Line 24). Fischer further states that if the signatures are not determined to be valid, then the routine braches to block 324 where the execution in program X is suppressed (Column 16 Line 64).

Fischer fails to teach wherein said other signature data is user signature data;

wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program,

However, Durst teaches user signature data , wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program [abstract, col. 3, lines 35-67, i.e. " signature of one or more authorized computer systems is determined and stored , and the, prior to executing a particular program intended to be installed in a computer system, the stored signature is compared to the signature of the computer system intended to be used],

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Fischer with the teaching of Durst to prevent computer program from being used by an unauthorized computer system [col. 1, lines 5-13].

As per claims 4, 25, and 46, Fischer as modified teach wherein said module signature data, said core signature data and said user signature data include public key infrastructure signatures.

Fischer teaches that the authorization signature includes a signature segment which may include a reference to the signer's certificate which contains the user's public key and name (Column 6 Line 23). Therefore it is determined that the signature data includes public key infrastructure signatures.

5. **Claims 1, 5-7, 16, 22, 26-28, 37, 43, 47-49, and 58** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,151,643 to Cheng in view of US Patent No. 5,113,518 to Durst, Jr. et al. (hereinafter " Durst).

Cheng teaches a method and system that automatically updates software components from numerous vendors on the computer systems of a plurality of end users (Column 2 Line 63). Cheng further teaches a computer-implemented method of providing information for software residing on a client computer (Column 25 Line 35).

As per claims 1, 22, and 43, Cheng teaches :

reading module signature data associated with said additional computer program module;

reading core signature data and other signature data associated with said core computer program;

comparing said module signature data with said core signature data and said other signature data" "Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data" Cheng teaches a method that automatically updates software components from numerous vendors on the computer systems of a plurality of end users (Column 2 Line 63). Cheng further teaches a step 203 where the registered users are authenticated by the service provider computer 102 using conventional authentication mechanisms such as digital signatures, certificates, or the like. Authentication ensures that only registered users who are properly authorized by the service provider can obtain software updates (Column 7 Line 40). Authentication of the software updates ensures that the software updates are virus free and uncorrupted (Abstract Line 26). Cheng teaches a security module 701 which handles the authentication of the users which may be implemented with conventional authentication mechanisms based on digital signatures, such as public key systems supporting digital signatures, certificates and the like (Column 16 Line 39). Cheng additionally teaches that the security module 701 provides for verification of the integrity of software updates that are downloaded from the software vendor to ensure that such updates have not been altered or infected by computer viruses or other modifications (Column 16 Line 48).

Cheng fails to teach wherein said other signature data is user signature data;

wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program,

However, Durst teaches user signature data , wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program [abstract, col. 3, lines 35-67, i.e. " signature of one or more authorized computer systems is determined and stored', and the, prior to executing a particular program intended to be installed in a computer system, the stored signature is compared to the signature of the computer system intended to be used],

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Cheng with the teaching of Durst to prevent computer program from being used by an unauthorized computer system [col. 1, lines 5-13].

As per claims 5, 26, and 47, Cheng as modified teaches wherein said user signature data is associated with said core computer program upon installation of said core computer program [Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35).

As per claims 6, 27, and 48, Cheng teaches wherein said user signature data is embedded within said core computer program [Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35)].

As per claims 7, 28, and 49, Cheng teaches wherein said user signature data is embedded within said core computer program by applying a user specific patch to said core computer program [Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35)].

As per claims 16, 37, and 58, Cheng teaches wherein said additional computer program module is operable to install another computer program [Cheng teaches that client application performs the installation, executing any necessary decompression, installation, or setup applications necessary to install the software update (Column 9 Line 3)].

6. **Claims 1, 22, and 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,157,721 to Shear in view of US Patent No. 5,113,518 to Durst, Jr. et al. (hereinafter " Durst).

Shear teaches a system and method using cryptography to protect secure computing environments (Column 1 Line 1).

As per claims 1, 22, and 43, Shear teaches:

reading module signature data associated with said additional computer program module [Shear teaches a method where a protected processing environment can distinguish between authorized and unauthorized load modules by examining the load module to see whether it bears the sea' of verifying authority (Column 9 Line 58). Shear further discloses that the digital sealing process is actually performed by creating a "digital signature" using a well-known process (Column 10 Line 58)].

reading core signature data and other signature data associated with said core computer program;

comparing said module signature data with said core signature data and said other signature data" Shear teaches that the protected processing environment compares the version of message digest it obtains from the digital signature with the version of message digest it calculates itself from the load module using the one way hash transformation (Column 14 Line 52).

refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data [Shear teaches that the message digests mentioned above should be identical. If they do not match, then digital signature 106 is not authentic or load module 54 has been changed and protected processing environment 108 rejects load module 54 (Column 14 Line 56)].

Shear fails to teach:

wherein said other signature data is user signature data;

wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program,

However, Durst teaches user signature data , wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program [abstract, col. 3, lines 35-67, i.e. " signature of one or more authorized computer systems is determined and stored , and the, prior to executing a particular program intended to be installed in a computer system, the stored signature is compared to the signature of the computer system intended to be used],

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Shear with the teaching of Durst to prevent computer program from being used by an unauthorized computer system [col. 1, lines 5-13].

7. **Claims 1, 10, 11, 13-15, 17-20, 22, 31, 32, 34-36, 38-41, 43, 52, 53, 55-57, and 59-62** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,108,420 to Larose in view of US Patent No. 5,113,518 to Durst, Jr. et al. (hereinafter " Durst).

Larose teaches a method and system for the electronic distribution and installation to users via a network (Column 1 Line 7).

As per claims 1, 22, and 43, Larose teaches:

reading module signature data associated with said additional computer program module [Larose teaches a step where the program examines the file to determine the location of the overall cryptographic signature, the embedded data cryptographic signature and embedded data (Column 12 Line 53)];

reading core signature data and other signature data associated with said core computer program [Larose teaches a step where a local version of the overall cryptographic signature is calculated using the same known cryptographic signature algorithm that was employed by the SDA 100 (Column 13 Line 1)]

comparing said module signature data with said core signature data and said other signature data [Larose teaches that the locally calculated overall fingerprint is compared to the decrypted remote overall fingerprint (Column 13 Line 9). Larose further teaches that the locally calculated embedded data fingerprint is compared to the decrypted remote embedded data fingerprint (Column 13 Line 27)];

refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data [Larose teaches that if either or both of the above mentioned comparison differ, then the authentication and reading program will fail with a warning that the installed aggregate distribution file has been corrupted (Column 13 Lines 11 and 29)];

Larose fails to teach:

wherein said other signature data is user signature data;

wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program,

However, Durst teaches user signature data , wherein the user signature data allows a particular user to authorize the additional computer program module for use with the installed computer program [abstract, col. 3, lines 35-67, i.e. " signature of one or more authorized computer systems is determined and stored , and the, prior to executing a particular program intended to be installed in a computer system, the stored signature is compared to the signature of the computer system intended to be used],

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Larose with the teaching of Durst to prevent computer program from being used by an unauthorized computer system [col. 1, lines 5-13].

As per claims 10, 31, and 52, Larose teaches wherein said core computer program is an anti-virus computer program [Larose teaches that the authentication and reading program may not be a standalone program and could be incorporated as functions of other programs such as a license checker or a virus-checker program (Column 12. Line 24)].

As per claims 11, 32, and 53, Larose teaches wherein said anti-virus computer program operates with at least one updateable anti-virus computer program module [Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25)].

As per claims 13, 34, and 55, Larose teaches wherein said additional computer program module provides functionality independent of that of said core computer program [Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25)].

As per claims 14, 35, and 56, Larose teaches wherein said additional computer program module does not relate to anti-virus protection" Larose teaches an example where the disclosed invention could be used in a computer game environment (Column 14 Line 47).

As per claims 15, 36, and 57, Larose teaches wherein said additional computer program is operable to patch an installed computer program" Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25)].

As per claims 17, 38, and 59, Larose teaches writing said additional computer program module [Larose teaches a step where an input/output logic 111 of the conversion program 110 reads in the desired original distribution file 130 (Column 7 Line 34). The office concludes that the original file was written at some point in time prior to this step];

receiving new user information from a new user of said additional computer program module [Larose teaches a User Installation Agent (UIA) 2_00 that accepts data 32 input from the user, such as name, address, payment options, etc. (Column 5 Line 21)];

generating user signature data specific to said new user in dependence upon said new user information [Larose teaches a step 2 which generates a cryptographic signature from the given user information (Column 7 Line 34)];

associating said user signature data with said additional computer program module [Larose teaches a Secure Distribution Agent (SDA) that combines identifying data, which constitutes information concerning the user, with the data stored in the databases to produce an aggregate distribution file that is uniquely customized, authenticable, and traceable to the user (Column 5 Line 43). Larose further teaches that the output of the conversion program 110 is an aggregate distribution file 170 which contains both the contents of the original distribution file 130, the embedded data 140, as well as a cryptographic signature of the embedded data an the original distribution file (Column 6 Line 27)];

providing said additional computer program module with associated user signature data to said new user [Larose teaches embedded data, which can include a unique serial number, used to identify the aggregate distribution file to be distributed to the user. The office concludes that the module is distributed to the user according to the disclosed invention (Column 6 Line 16)].

As per claims 18, 39, and 60, Larose teaches wherein said step of generating uses a tool produced by a provider of said core computer program [Larose teaches a conversion program 110 that is used in generating the user signature data. It is clearly illustrated in Figure 2 that the conversion program is part of the SDA].

As per claims 19, 40, and 61, Larose teaches wherein said step of associating uses a tool produced by a provider of said core computer program [Larose teaches a Secure Distribution Agent (SDA) mentioned above that is used in the associating process. Larose teaches that the SDA is resident on a distribution computer that is an essential part of the disclosed invention (Column 4 Line 34)].

As per claims 20, 41, and 62, Larose teaches writing said additional computer program module [Larose teaches a step where an input/output logic 111 of the conversion program 110 reads in the desired original distribution file 130 (Column 7 Line 34). The office concludes that the original file was written at some point in time prior to this step];

generating signature data specific to said additional computer program module in dependence upon said additional computer program module using a tool produced by a provider of said core computer program [Larose teaches a step 2 which generates a cryptographic signature from the given user information (Column 7 Line 34)];

associating said signature data with said additional computer program module [Larose teaches a Secure Distribution Agent (SDA) that combines identifying data, which constitutes information concerning the user, with the data stored in the databases to produce an aggregate distribution file that is uniquely customized, authenticable, and traceable to the user (Column 5 Line .43). Larose further teaches that the output of the conversion program 110 is an aggregate distribution file 170 which contains both the contents of the original distribution file 130, the embedded data 140, as well as a cryptographic signature of the embedded data an the original distribution file (Column 6 Line 27)];

providing said additional computer program module with associated signature data to said new user [Larose teaches embedded data, which can include a unique serial number, used to identify the aggregate distribution file to be distributed to the user. The office concludes that the module is distributed to the user according to the disclosed invention (Column 6 Line 16)].

Allowable Subject Matter

8. Claims 64-66 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Action is Final

9. **THIS ACTION IS FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. A.
Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100